Claims

1. A method for accessing a data processing system (D1), which is formed from data processing units (1, 2, 3) which are networked to one another for the exchange of data, having the following steps:

providing a first authentication means (9) for authenticating a system administrator (4),

authenticating the system administrator (4) on a first data processing unit (1) by transferring the first authentication means (9) to an authentication program (5),

providing a second authentication means (10) for authenticating a system technician (8),

authenticating the system technician (8) on a second data processing unit (7) by transferring the second authentication means (10) to the authentication program (5) and resulting automatic generation of an identification information item which identifies the carrier of the second authentication means (10),

displaying the identification information item on the first data processing unit (1) of the system administrator (4), and

enabling access authorization for the system technician (8) and automatic triggering of a function for generating and storing a log file which logs the activity of the system technician (8) on the data processing system (D1).

2. The method as claimed in claim 1, wherein the second authentication means (10) is compared by means of the authentication program (5) by accessing a file which contains verified, second authentication means (10), and when there is correspondence with one of the verified, second authentication means (10) a corresponding information item is transferred to the system administrator (4).

3. The method as claimed in claim 2, wherein each verified, second authentication means (10) contained in the file is assigned an identification information item which is specific thereto.

4. The method as claimed in claim 3, wherein the identification information item comprises the name and, if appropriate, the membership of the system technician (8) of a specific organization.

5. A method for accessing a data processing system (D1) which is formed from data processing units (1, 2, 3) which are networked to one another for the exchange of data, having the following steps:

providing a first authentication means (9) for authenticating a system administrator (4),

authenticating the system administrator (4) on a first data processing unit (1) by transferring the first authentication means (9) to an authentication program (5),

providing a second authentication means (10) for authenticating a system technician (8),

authenticating the system technician (8) on a second data processing unit (7) by transferring the second

authentication means (10) to the authentication program (5) and resulting automatic generation of an identification information item which identifies the carrier of the second authentication means (10),

the first authentication means (9) and/or the second authentication means (10) being an authentication code which can be transferred to the authentication program (5) preferably by means of a keypad which is provided on a data processing unit (1, 7),

displaying the identification information item on the first data processing unit (1) of the system administrator (4), and

enabling access authorization for the system technician (8) and automatic triggering of a function for generating and storing a log file which logs the activity of the system technician (8) on the data processing system (D1).

6. The method as claimed in claim 5, wherein the authentication code is stored in a mobile memory unit which can be connected to the data processing system (D1, D2) for the transmission of data.

7. The method as claimed in claim 6, wherein the memory unit is an authentication card (9, 10) which is provided with a data carrier.

8. The method as claimed in claim 7, wherein the authentication card (9, 10) has a memory means, in particular for storing the log file, and/or an information item which permits access to the log file.

9. A method for accessing a data processing system (D1), which is formed from data processing units (1, 2, 3) which are networked to one another for the exchange of data, having the following steps:

providing a first authentication means (9) for authenticating a system administrator (4),

authenticating the system administrator (4) on a first data processing unit (1) by transferring the first authentication means (9) to an authentication program (5),

providing a second authentication means (10) for authenticating a system technician (8),

authenticating the system technician (8) on a second data processing unit (7) by transferring the second authentication means (10) to the authentication program (5) and resulting automatic generation of an identification information item which identifies the carrier of the second authentication means (10),

displaying the identification information item on the first data processing unit (1) of the system administrator (4), and

enabling access authorization for the system technician (8) and automatic triggering of a function for generating and storing a log file which logs the activity of the system technician (8) on the data processing system (D1),

wherein the enabling of an access authorization is done via the system administrator (4) by manually triggering a function which is provided for this purpose in the authentication program (5), and

can be accessed exclusively by the system administrator (8).

10. The method as claimed in one of the preceding claims, wherein the data processing system (D1) processes data which can be accessed

by an individual person only with particular authorization,

or

only by persons with a simple authorization according to the two man principle when the particular authorization is not present.

11. The method as claimed in claim 10, wherein proof of the particular authorization is given by transferring a third authentication means, assigned to the person, to the data processing system (D1).

12. The method as claimed in claim 10, wherein the data is personal data which requires protection, in particular patient data.

13. The method as claimed in claim 1, wherein the connection between the first data processing unit (1) and the second data processing unit (7) is established via the Internet or via an Intranet.